CLAIMS

WHAT IS CLAIMED IS:

1. A method of securely accessing data in a personal computer, the method comprising:

reading a secret from a first location;

securing the secret in a secure location different from the first location; and

retrieving at least a portion of the data stored in the first location using the secret.

2. The method of claim 1, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory; and

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret.

3. The method of claim 2, wherein the memory is a read-only memory (ROM);

wherein reading a secret from the memory comprises reading the secret from the ROM;

wherein securing the secret in a secure location different from the memory comprises securing the secret in the secure location different from the ROM; and

wherein retrieving at least a portion of the data stored in the memory using the secret comprises retrieving at least the portion of the data stored in the ROM using the secret.

4. The method of claim 3, wherein the data comprises basic input-output system (BIOS) data and the ROM is a BIOS ROM configured to store the BIOS data;

wherein reading the secret from the ROM comprises reading the secret from the BIOS ROM;

wherein securing the secret in the secure location different from the ROM comprises securing the secret in the secure location different from the BIOS ROM; and

wherein retrieving at least a portion of the data stored in the ROM using the secret comprises retrieving at least a portion of the BIOS data stored in the BIOS ROM using the secret.

5. The method of claim 3, wherein reading the secret from the ROM comprises reading the secret from within the data stored within the ROM.

6. The method of claim 1, further comprising:

reading code from the first location, wherein the code is different from the secret and different from the data stored in the first location;

wherein retrieving at least a portion of the data stored in the first location using the secret comprises retrieving at least a portion of the data stored in the first location using the code and the secret.

7. The method of claim 6, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret;

wherein reading code from the first location comprises reading code from the memory wherein the code is different from the secret and different from the data stored in the memory; and

wherein retrieving at least the portion of the data stored in the first location using the code and the secret comprises retrieving at least a portion of the data stored in the memory using the code and the secret.

8. The method of claim 7, wherein reading the secret within the memory and reading code from the memory further comprises reading the secret from inside the code within the memory.

9. The method of claim 6, further comprising:

unlocking a lock bit associated with the data stored in the first location prior to retrieving at least the portion of the data stored in the first location using the secret.

10. The method of claim 9, wherein the location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret;

wherein reading code from the first location comprises reading code from the memory wherein the code is different from the secret and different from the data stored in the memory;

wherein retrieving at least the portion of the data stored in the first location using the code and the secret comprises retrieving at least a portion of the data stored in the memory using the code and the secret; and

wherein unlocking the lock bit associated with the data stored in the first location prior to retrieving at least the portion of the data stored in the first location using the secret comprises unlocking the lock bit associated with the data stored in the memory prior to retrieving at least the portion of the data stored in the memory using the secret.

11. The method of claim 9, further comprising:

processing the secret using the code;

wherein unlocking a lock bit associated with the data stored in the first location comprises unlocking the lock bit associated with the data stored in the first location in response to processing the secret using the code.

12. The method of claim 11, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret;

wherein reading code from the first location comprises reading code from the memory, wherein the code is different from the secret and different from the data stored in the memory;

wherein retrieving at least the portion of the data stored in the first location using the code and the secret comprises retrieving at least a portion of the data stored in the memory using the code and the secret;

wherein unlocking the lock bit associated with the data stored in the first location prior to retrieving at least the portion of the data stored in the first location using the secret comprises unlocking the lock bit associated with the data stored in the memory prior to retrieving at least the portion of the data stored in the memory using the secret; and

wherein unlocking the lock bit associated with the data stored in the first location comprises unlocking the lock bit associated with the data stored in the memory in response to processing the secret using the code.

13. The method of claim 1, further comprising:

unlocking a lock bit associated with data stored in the first location prior to retrieving at least the portion of the data stored in the first location using the secret.

14. The method of claim 13, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret; and

wherein unlocking a lock bit associated with data stored in the first location prior to retrieving at least the portion of the data stored in the first location using the secret comprises unlocking a lock bit associated with data stored in the memory prior to retrieving at least the portion of the data stored in the memory using the secret.

15. The method of claim 1, further comprising:

storing the secret within the first location securely;

storing data within the first location securely; and

storing code different from the secret and different from the data within the first location securely.

16. The method of claim 15, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret;

wherein storing the secret within the first location securely comprises storing the secret within the memory securely;

wherein storing data within the first location securely comprises storing data within the memory securely; and

wherein storing code different from the secret and different from the data within the first location securely comprises storing code different from the secret and different from the data within the memory securely

17. The method of claim 16, wherein the memory is a read-only memory (ROM);

wherein storing a secret within the memory comprises storing a secret within the ROM;

wherein storing data within the memory comprises storing data within the ROM;

wherein storing code different from the secret and different from the data within the memory comprises storing code different within secret and different from the data within the ROM;

wherein securing the secret in a secure location different from the memory comprises securing the secret in a secure location different from the ROM; and

wherein retrieving at least a portion of the data from the memory using the secret comprises retrieving at least a portion of the data from the ROM using the secret.

18. The method of claim 17, wherein the data comprises basic input-output system (BIOS) data and the ROM is a BIOS ROM configured to store the BIOS data;

wherein storing a secret within the ROM comprises storing a secret within the BIOS ROM;

wherein storing data within the ROM comprises storing data within the BIOS ROM;

wherein storing code different within secret and different from the data within the ROM comprises storing code different within secret and different from the BIOS data within the BIOS ROM;

wherein securing the secret in a secure location different from the ROM comprises securing the secret in a secure location different from the BIOS ROM; and

wherein retrieving at least a portion of the data from the ROM using the secret comprises retrieving at least a portion of the BIOS data from the BIOS ROM using the secret.

19. The method of claim 16, wherein storing a secret within the memory and storing data within the memory comprises storing the secret inside the data within the memory.

20. The method of claim 16, wherein storing a secret within the memory and storing code different from the secret and different from the data within the memory comprises storing the secret inside the code within the memory.

21. The method of claim 16, further comprising:

unlocking a lock bit associated with the data prior to retrieving at least the portion of the data from the memory using the secret.

22. The method of claim 21, further comprising:

reading the code from the memory; and

securing the code in a secure location different from the memory;

wherein retrieving at least a portion of the data from the memory using the secret comprises retrieving at least a portion of the data from the memory using the code and the secret.

23. The method of claim 22, wherein reading the secret from the memory comprises reading the secret from the memory during a boot sequence; and

wherein securing the secret in a secure location different from the memory comprises storing the secret in SMM memory space.

24. The method of claim 22, wherein retrieving at least a portion of the data from the memory using the code and the secret further comprises:

processing the code; and

transmitting at least an indication of the secret to the memory;

25. The method of claim 24, wherein retrieving at least a portion of the data from the memory using the code and the secret further comprises:

receiving a challenge from the memory; and

transmitting a response to the memory including at least an indication of the secret to the memory, in response to receiving the challenge.

26. The method of claim 1, further comprising:

reading the code from the first location; and

securing the code in a secure location different from the first location;

wherein retrieving at least a portion of the data from the first location using the secret comprises retrieving at least a portion of the data from the first location using the code and the secret.

27. The method of claim 26, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret;

wherein reading the code from the reading the code from the memory comprises reading the code from the memory;

wherein securing the code in a secure location different from the first location comprises securing the code in a secure location different from the memory; and

wherein retrieving at least a portion of the data from the first location using the secret further comprises retrieving at least a portion of the data from the memory using the code and the secret.

28. The method of claim 1, wherein reading the secret from the first location comprises reading the secret from the first location during a boot sequence; and

wherein securing the secret in a secure location different from the first location comprises storing the secret in SMM memory space.

29. The method of claim 28, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from a memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret; and

wherein reading the secret from the memory further comprises reading the secret from the memory during a boot sequence.

30. The method of claim 1, further comprising:

providing a lock bit associated with the data that when set provides an indication that the data stored in the memory is secured.

31. The method of claim 30, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret; and

wherein providing the lock bit associated with the data that when set provides an indication that the data stored in the first location is secured comprises providing a lock bit associated with the data that when set provides an indication that the data stored in the memory is secured

32. A method of securing data in a personal computer system, the method comprising:

storing a secret within a first location; and

storing code different from the secret within the first location;

wherein the code is configured to provide access to data stored in the first location when processed in association with the secret.

33. The method of claim 32, wherein the first location comprises a memory;

wherein storing the secret within the first location comprises storing a secret within the memory;

wherein storing code different from the secret within the first location comprises storing code different from the secret within the memory; and

wherein the code is configured to provide access to data stored in the first location when processed in association with the secret further comprises the code being configured to provide access to data stored in the memory when processed in association with the secret.

34. The method of claim 33, wherein the memory is a read-only memory (ROM);

wherein storing a secret within the memory comprises storing a secret within the ROM; and

wherein storing code different from the secret within the memory comprises storing code different within secret within the ROM; and

wherein the code is configured to provide access to data stored in the ROM when processed in association with the secret.

35. The method of claim 34, wherein the data comprises basic input-output system (BIOS) data and the ROM is a BIOS ROM configured to store the BIOS data;

wherein storing a secret within the ROM comprises storing a secret within the BIOS ROM;

wherein storing code different within secret within the ROM comprises storing code different within secret within the BIOS ROM; and

wherein the code is configured to provide access to BIOS data stored in the BISO ROM when processed in association with the secret.

36. The method of claim 33, wherein storing a secret within the memory comprises storing the secret inside the data within the memory.

37. The method of claim 33, wherein storing a secret within the memory and storing code different from the secret within the memory comprises storing the secret inside the code within the memory.

38. The method of claim 33, further comprising:

providing a lock bit associated with the data stored in the memory that when set provides an indication that the data stored in the memory is secured.

39. A personal computer system, comprising:

a first location configured to store code, a secret, and data different from the secret and different from the code;

a master device operably coupled to the first location, wherein the master device is configured to read the secret from the first location and to store the secret in a secure location different from the first location, and wherein the master device is further configured to access the data stored in the first location using the secret.

40. The personal computer system of claim39, wherein the first location comprises a memory.

41. The personal computer system of claim 40, wherein the memory comprises a read-only memory (ROM).

42. The personal computer system of claim 41, wherein the ROM comprises a basic input-output system (BIOS) ROM, and wherein the data comprise BIOS data.

43. The personal computer system of claim 41, wherein the master device is further configured to read the secret from within the data stored within the ROM.

44. The computer system of claim 41, wherein the master device is further configured to read the code from the memory; and wherein the master device is further configured to retrieve at least a portion of the data stored in the memory using the code and the secret.

45. The computer system of claim 39, further comprising:

a lock bit associated with the data stored in the first location; and

wherein the master device is further configured to unlock the lock bit associated with the data stored in the first location.

46. The personal computer system of claim 45, wherein the first location comprises a memory.

47. The computer system of claim 46, wherein the master device is further configured to process the secret using the code; and wherein the master device is further configured to unlock the lock bit associated with the data stored in the memory in response to processing the secret using the code.

48. The computer system of claim 47, wherein the master device is further configured to receive a challenge from the memory and to transmit a response to the memory including at least an indication of the secret to the memory, in response to receiving the challenge.

49. The computer system of claim 39, wherein the master device is further configured to read the secret from the first location during a boot sequence; and wherein the master device is further configured to store the secret in SMM memory space.

50. The computer system of claim 39, wherein the master device includes a microprocessor.

51. A personal computer system, comprising:

means for securely storing data;

means for reading a secret from the means for securely storing data;

means for securing the secret in a secure location different from the means for securely storing data; and

means for retrieving at least a portion of the data stored in the means for securely storing data using the secret.

52. The personal computer system of claim 51, further comprising:

means for reading code from the means for securely storing data, wherein the code is different from the secret and different from the data stored in the means for securely storing data;

wherein the means for retrieving at least a portion of the data stored in the means for securely storing data from the means for securely storing data using the secret comprises means for retrieving at least a portion of the data stored in the means for securely storing data using the code and the secret.

53. The personal computer system of claim 51, further comprising:

means for locking the means for securely storing data; and

means for unlocking the means for locking.

54. The personal computer system of claim 51, further comprising:

means for processing the secret using the code.

55. A method of securely accessing data in a personal computer, the method comprising:

step for reading a secret from a first location;

step for securing the secret in a secure location different from the first location; and

step for retrieving at least a portion of the data stored in the first location using the secret.

56. The method of claim 55, further comprising:

step for reading code from the first location, wherein the code is different from the secret and different from the data stored in the first location;

wherein the step for retrieving at least the portion of the data stored in the first location using the secret comprises step for retrieving at least the portion of the data stored in the first location using the code and the secret.

57. The method of claim 55, further comprising:

step for unlocking a lock bit associated with the data stored in the first location prior to the step for retrieving at least the portion of the data stored in the first location using the secret.

58. The method of claim 57, further comprising:

step for processing the secret using the code;

wherein the step for unlocking the lock bit associated with the data stored in the first location comprises step for unlocking the lock bit associated with the data stored in the first location in response to the step for processing the secret using the code.

59. The method of claim 55, further comprising:

step for storing the secret within the first location securely;

step for storing data within the first location securely; and

step for storing code different from the secret and different from the data within the first location securely.

60. The method of claim 59, further comprising:

step for unlocking a lock bit associated with the data prior to the step for retrieving at least the portion of the data from the first location using the secret.

61. The method of claim 60, further comprising:

step for reading the code from the first location; and

step for securing the code in a secure location different from the first location;

wherein the step for retrieving at least the portion of the data from the first location using the secret comprises step for retrieving at least the portion of the data from the first location using the code and the secret.

62. The method of claim 55, further comprising:

step for reading the code from the first location; and

step for securing the code in a secure location different from the first location;

wherein the step for retrieving at least the portion of the data from the first location using the secret comprises step for retrieving at least a portion of the data from the first location using the code and the secret.

63. The method of claim 55, further comprising:

step for providing a lock bit associated with the data that when set provides an indication that the data stored in the first location is secured.

64. A method of securing data in a personal computer system, the method comprising:

step for storing a secret within a first location; and

step for storing code different from the secret within the first location;

wherein the code is configured to provide access to data stored in the first location when processed in association with the secret.

65. The method of claim 64, further comprising:

step for providing a lock bit associated with the data stored in the first location that when set provides an indication that the data stored in the first location is secured.

66. A computer readable program storage device encoded with instructions that, when executed by a personal computer, performs a method of securely accessing data in the personal computer, the method comprising:

reading a secret from a first location;

securing the secret in a secure location different from the first location; and

retrieving at least a portion of the data stored in the first location using the secret.

67. The computer readable program storage device of claim 66, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory; and

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret.

68. The computer readable program storage device of claim 67, wherein the memory is a read-only memory (ROM);

wherein reading a secret from the memory comprises reading the secret from the ROM;

wherein securing the secret in a secure location different from the memory comprises securing the secret in the secure location different from the ROM; and

wherein retrieving at least a portion of the data stored in the memory using the secret comprises retrieving at least the portion of the data stored in the ROM using the secret.

69. The computer readable program storage device of claim 68, wherein the data comprises basic input-output system (BIOS) data and the ROM is a BIOS ROM configured to store the BIOS data;

wherein reading the secret from the ROM comprises reading the secret from the BIOS ROM;

wherein securing the secret in the secure location different from the ROM comprises securing the secret in the secure location different from the BIOS ROM; and

wherein retrieving at least a portion of the data stored in the ROM using the secret comprises retrieving at least a portion of the BIOS data stored in the BIOS ROM using the secret.

70. The computer readable program storage device of claim 68, wherein reading the secret from the ROM comprises reading the secret from within the data stored within the ROM.

71. The computer readable program storage device of claim 66, the method further comprising:

reading code from the first location, wherein the code is different from the secret and different from the data stored in the first location;

wherein retrieving at least a portion of the data stored in the first location using the secret comprises retrieving at least a portion of the data stored in the first location using the code and the secret.

72. The computer readable program storage device of claim 71, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret;

wherein reading code from the first location comprises reading code from the memory wherein the code is different from the secret and different from the data stored in the memory; and

wherein retrieving at least the portion of the data stored in the first location using the code and the secret comprises retrieving at least a portion of the data stored in the memory using the code and the secret.

73. The computer readable program storage device of claim 72, wherein reading the secret within the memory and reading code from the memory further comprises reading the secret from inside the code within the memory.

74. The computer readable program storage device of claim 71, the method further comprising:

unlocking a lock bit associated with the data stored in the first location prior to retrieving at least the portion of the data stored in the first location using the secret.

75. The computer readable program storage device of claim 74, wherein the location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret;

wherein reading code from the first location comprises reading code from the memory wherein the code is different from the secret and different from the data stored in the memory;

wherein retrieving at least the portion of the data stored in the first location using the code and the secret comprises retrieving at least a portion of the data stored in the memory using the code and the secret; and

wherein unlocking the lock bit associated with the data stored in the first location prior to retrieving at least the portion of the data stored in the first location using the secret comprises unlocking the lock bit associated with the data stored in the memory prior to retrieving at least the portion of the data stored in the memory using the secret.

76. The computer readable program storage device of claim 74, the method further comprising:

processing the secret using the code;

wherein unlocking a lock bit associated with the data stored in the first location comprises unlocking the lock bit associated with the data stored in the first location in response to processing the secret using the code.

77. The computer readable program storage device of claim 76, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret;

wherein reading code from the first location comprises reading code from the memory, wherein the code is different from the secret and different from the data stored in the memory;

wherein retrieving at least the portion of the data stored in the first location using the code and the secret comprises retrieving at least a portion of the data stored in the memory using the code and the secret;

wherein unlocking the lock bit associated with the data stored in the first location prior to retrieving at least the portion of the data stored in the first location using the secret comprises unlocking the lock bit associated with the data stored in the memory prior to retrieving at least the portion of the data stored in the memory using the secret; and

wherein unlocking the lock bit associated with the data stored in the first location comprises unlocking the lock bit associated with the data stored in the memory in response to processing the secret using the code.

78. The computer readable program storage device of claim 66, the method further comprising:

unlocking a lock bit associated with data stored in the first location prior to retrieving at least the portion of the data stored in the first location using the secret.

79. The computer readable program storage device of claim 78, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret; and

wherein unlocking a lock bit associated with data stored in the first location prior to retrieving at least the portion of the data stored in the first location using the secret comprises unlocking a lock bit associated with data stored in the memory prior to retrieving at least the portion of the data stored in the memory using the secret.

80. The computer readable program storage device of claim 66, further comprising:

storing the secret within the first location securely;

storing data within the first location securely; and

storing code different from the secret and different from the data within the first location securely.

81. The computer readable program storage device of claim 80, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret;

wherein storing the secret within the first location securely comprises storing the secret within the memory securely;

wherein storing data within the first location securely comprises storing data within the memory securely; and

wherein storing code different from the secret and different from the data within the first location securely comprises storing code different from the secret and different from the data within the memory securely

82. The computer readable program storage device of claim 81, wherein the memory is a read-only memory (ROM);

wherein storing a secret within the memory comprises storing a secret within the ROM;

wherein storing data within the memory comprises storing data within the ROM;

wherein storing code different from the secret and different from the data within the memory comprises storing code different within secret and different from the data within the ROM;

wherein securing the secret in a secure location different from the memory comprises securing the secret in a secure location different from the ROM; and

wherein retrieving at least a portion of the data from the memory using the secret comprises retrieving at least a portion of the data from the ROM using the secret.

83. The computer readable program storage device of claim 82, wherein the data comprises basic input-output system (BIOS) data and the ROM is a BIOS ROM configured to store the BIOS data;

wherein storing a secret within the ROM comprises storing a secret within the BIOS ROM;

wherein storing data within the ROM comprises storing data within the BIOS ROM;

wherein storing code different within secret and different from the data within the ROM comprises storing code different within secret and different from the BIOS data within the BIOS ROM;

wherein securing the secret in a secure location different from the ROM comprises securing the secret in a secure location different from the BIOS ROM; and

wherein retrieving at least a portion of the data from the ROM using the secret comprises retrieving at least a portion of the BIOS data from the BIOS ROM using the secret.

84. The computer readable program storage device of claim 81, wherein storing a secret within the memory and storing data within the memory comprises storing the secret inside the data within the memory.

85. The computer readable program storage device of claim 81, wherein storing a secret within the memory and storing code different from the secret and different from the data within the memory comprises storing the secret inside the code within the memory.

86. The computer readable program storage device of claim 81, further comprising:

unlocking a lock bit associated with the data prior to retrieving at least the portion of the data from the memory using the secret.

87. The computer readable program storage device of claim 86, further comprising:

reading the code from the memory; and

securing the code in a secure location different from the memory;

wherein retrieving at least a portion of the data from the memory using the secret comprises retrieving at least a portion of the data from the memory using the code and the secret.

88. The computer readable program storage device of claim 87, wherein reading the secret from the memory comprises reading the secret from the memory during a boot sequence; and

wherein securing the secret in a secure location different from the memory comprises storing the secret in SMM memory space.

89. The computer readable program storage device of claim 87, wherein retrieving at least a portion of the data from the memory using the code and the secret further comprises:

processing the code; and

transmitting at least an indication of the secret to the memory;

90. The computer readable program storage device of claim 89, wherein retrieving at least a portion of the data from the memory using the code and the secret further comprises:

receiving a challenge from the memory; and

transmitting a response to the memory including at least an indication of the secret to the memory, in response to receiving the challenge.

91. The computer readable program storage device of claim 66, further comprising:

reading the code from the first location; and

securing the code in a secure location different from the first location;

wherein retrieving at least a portion of the data from the first location using the secret comprises retrieving at least a portion of the data from the first location using the code and the secret.

92. The computer readable program storage device of claim 91, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret;

wherein reading the code from the reading the code from the memory comprises reading the code from the memory;

wherein securing the code in a secure location different from the first location comprises securing the code in a secure location different from the memory; and

wherein retrieving at least a portion of the data from the first location using the secret further comprises retrieving at least a portion of the data from the memory using the code and the secret.

93. The computer readable program storage device of claim 66, wherein reading the secret from the first location comprises reading the secret from the first location during a boot sequence; and

wherein securing the secret in a secure location different from the first location comprises storing the secret in SMM memory space.

94. The computer readable program storage device of claim 93, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from a memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret; and

wherein reading the secret from the memory further comprises reading the secret from the memory during a boot sequence.

95. The computer readable program storage device of claim 66, further comprising:

providing a lock bit associated with the data that when set provides an indication that the data stored in the memory is secured.

96. The computer readable program storage device of claim 95, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret; and

wherein providing the lock bit associated with the data that when set provides an indication that the data stored in the first location is secured comprises providing a lock bit associated with the data that when set provides an indication that the data stored in the memory is secured

97. A computer readable program storage device encoded with instructions that, when executed by a personal computer system, performs a method of securing data in the personal computer system, the method comprising:

storing a secret within a first location; and

storing code different from the secret within the first location;

wherein the code is configured to provide access to data stored in the first location when processed in association with the secret.

98. The computer readable program storage device of claim 97, wherein the first location comprises a memory;

wherein storing the secret within the first location comprises storing a secret within the memory;

wherein storing code different from the secret within the first location comprises storing code different from the secret within the memory; and

wherein the code is configured to provide access to data stored in the first location when processed in association with the secret further comprises the code being configured to provide access to data stored in the memory when processed in association with the secret.

99. The computer readable program storage device of claim 98, wherein the memory is a read-only memory (ROM);

wherein storing a secret within the memory comprises storing a secret within the ROM; and

wherein storing code different from the secret within the memory comprises storing code different within secret within the ROM; and

wherein the code is configured to provide access to data stored in the ROM when processed in association with the secret.

100. The computer readable program storage device of claim 99, wherein the data comprises basic input-output system (BIOS) data and the ROM is a BIOS ROM configured to store the BIOS data;

wherein storing a secret within the ROM comprises storing a secret within the BIOS ROM;

wherein storing code different within secret within the ROM comprises storing code different within secret within the BIOS ROM; and

wherein the code is configured to provide access to BIOS data stored in the BISO ROM when processed in association with the secret.

101. The computer readable program storage device of claim 98, wherein storing a secret within the memory comprises storing the secret inside the data within the memory.

102. The computer readable program storage device of claim 98, wherein storing a secret within the memory and storing code different from the secret within the memory comprises storing the secret inside the code within the memory.

103. The computer readable program storage device of claim 98, further comprising:

providing a lock bit associated with the data stored in the memory that when set provides an indication that the data stored in the memory is secured.

5